210 N. Park Ave
Winter Park, FL
32789

P.O. Drawer 200
Winter Park, FL
32790-0200

Tel: 407-740-8575
Fax: 407-740-0613
tmi@tminc.com

February 5, 2007
Via Overnight Delivery

Secretary
Federal Communications Commission
Attention: CALEA Monitoring Report
445 12th Street, S.W.
Washington, D.C. 20554

RE: EasyTEL Communications Carrier Corporation
CALEA System Security and Integrity (SSI) Compliance Manual
Docket No. 04-295

Dear Secretary:

Attached please find the original and four (4) copies of the CALEA System Security and Integrity Compliance Manual, filed on behalf of EasyTEL Communications Carrier Corporation. This plan is filed as required of carrier offering VOIP services to end users. The company understands this document will be treated as presumptively confidential pursuant to the Commission's rules, 47 C.F.R § 0.459 and is therefore filed under seal.

Please acknowledge receipt of this filing by date stamping the extra copy of this cover letter and returning it to me in the self-addressed, stamped envelope provided.

Any questions you may have pertaining to this filing may be directed to me at (407) 740-3005 or via email at mbyrnes@tminc.com. Thank you for your assistance.

Sincerely,

Monique Byrnes
Consultant to EasyTEL

enclosure
cc: T.E. Kloehr
Easytel

cc: David Ward
FCC Senior Legal Advisor
Policy Division
Public Safety & Homeland Security Bureau
445 12th Street, SW
Washington DC 20554

file: EasyTEL - FCC
tms: CALEA 2007

No. of Copies rec'd 0+4
List A B C D E

CALEA System Security and Integrity Compliance Manual

for

Easytel Communications Carrier Corporation

Issued: February 5, 2007

I. DEFINITIONS

Appropriate legal authorization – means (1) a court order signed by a judge or magistrate authorizing or approving interception of wire or electronic communications; or (2) other authorization pursuant to 18 USC 2518(7), or any other relevant federal or state statute.

Appropriate carrier authorization – means the policies and procedures adopted by telecommunications carriers to supervise and control offers and employees authorized to assist law enforcement in conducting any interception of communications or access to call-identifying information.

Appropriate authorization – means both appropriate legal authorization and appropriate carrier authorization.

Call content interception – an interception of a communication, including its content (e.g., a wiretap carried out pursuant to a court order issued in accordance with Tile III).

Call information interception – accessing dialing or signaling information that identifies the origin, direction, destination, or termination of a communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier (e.g., a pen register or trap-and-trace surveillance under 18 USC §3121).

Carrier – a person engaged in the transmission or switching of wire or electronic communication as a common carrier for hire (including commercial mobile service) except insofar as the person is engaged in providing information services.

Easytel - Refers to Easytel Communications Carrier Corporation, issuer of this document.

Electronic surveillance – the implementation of either a call content interception or a call information interception.

FISA – The Foreign Intelligence Surveillance Act which is the federal statute that sets forth the minimum legal requirements for all electronic surveillance to acquire foreign intelligence information for periods up to one year. FISA is codified at 18 USC §1801.

LEA - Law Enforcement Agency; eg: Homeland Security, the Federal Bureau of Investigation or a state or local police department.

NeuStar - Refers to NeuStar, Inc., TTP for the Company.

Title III – Tile III of the Omnibus Crime Control and safe Streets Act of 1968, which is the federal statute that sets minimum legal requirements for all call content interceptions by government official and private citizens (except for those interceptions authorized under the Foreign Intelligence Surveillance Act). Title III is codified at 18 U.S.C. § 2510.

Trusted Third Party ("TTP") - An organization which would operate a service bureau with a system that has access to a carrier's network equipment and remotely manage the intercept process for the carrier.

II. STATEMENT OF CORPORATE POLICY

It is the policy of **Easytel Communications Carrier Corporation** to comply with the letter and spirit of all laws of the United States, including the Communications Assistance for Law Enforcement Act ("CALEA"). Section 105 of CALEA requires a telecommunication carrier to ensure, before assisting a law enforcement agency to carry out a call content interception or a call information interception, that the interception is activated (1) pursuant to court order or "other lawful authorization," and (2) with the "affirmative intervention" of a carrier officer or employee. 47 U.S.C. §1004. The Federal Communication Commission has issued regulations to implement Section 105 of the Act, which regulations are codified at 47 C.F.R. § 64.2100-2106. The FCC's regulations require that carriers create policies and procedures to govern their electronic surveillance activities. This Compliance Manual constitutes the required policies and procedures for **Easytel Communications Carrier Corporation.**

All employees are required to follow the policies and procedures specified in this manual. The FCC is authorized under CALEA to punish violations of both its regulations and carriers' internal surveillance policies and procedures. In addition, Tile 18 of the United States Code authorizes civil damages, fines, and imprisonment for the unlawful interception or disclosure of wire and electronic communications.

- Any questions about how to comply with policies and procedures in this manual should be referred to **T.E. Kloehr.**

- Any violation of or departure from the policies and procedures in this manual shall be reported immediately to **T.E. Kloehr.**

- Any compensation received as reimbursement for the expenses incurred in providing facilities and assistance pursuant to the policies and procedures in this manual (to the extent such are allowed by law) shall be reported or provided to **T.E. Kloehr.**

III. GENERAL POLICIES FOR ELECTRONIC SURVEILLANCE

A. "Appropriate Authorization" Required to Conduct Electronic Surveillance.

It is the policy of **Easytel Communications Carrier Corporation** to permit only lawful authorized electronic surveillance to be conducted on its premises.

Employees shall have both "appropriate legal authorization" and "appropriate carrier authorization" before enabling law enforcement officials and carrier personnel to implement the interception of communications or to access call-identifying information. Section IV of this Compliance Manual sets forth how each form of authorization is to be obtained.

B. Employees Designated as Points of Contact

Easytel Communications Carrier Corporation hereby designates the following senior officers or employees to serve as points of contact for the law enforcement agencies and provide appropriate carrier authorization. The employee(s) shall be available to law enforcement agencies during the times listed below, so that law enforcement agencies will always be able to contact at least one employee 24 hours a day, 7 days a week. If an employee cannot be available at a designated time, that employee shall arrange for one of other employees listed below to be available during that time.

Name or Position	Days and Times Available.	Telephone Number (s)
T.E. Kloehr President	**24 / 7**	**918-523-8010**
Ben Hilborn	**24 / 7**	**918-523-8005**
Darren Stolz	**24 / 7**	**918-523-8018**

Note: Wireline telephone calls are forwarded automatically to wireless telephone for 24 x 7 coverage.

III. GENERAL POLICIES FOR ELECTRONIC SURVEILLANCE, (CONT'D.)

C. Job Description for Designated Employees

1. The employee(s) designated in Section III.B above are hereby authorized by **Easytel Communications Carrier Corporation** to implement lawful electronic surveillance in accordance with the policies and procedures in this manual, to give appropriate carrier authorization and to delegate any tasks associated with the surveillance to other employees or a Trusted Third Party.

2. An employee designated in Section III.B above shall:

- Oversee the implementation of each electronic surveillance conducted on the premises of **Easytel Communications Carrier Corporation.**
- Coordinate and oversee the implementation of each electronic surveillance conducted on the premises of a TTP.
- Be responsible for assuring that he/she is fully apprised of all relevant state and federal statutory provisions affecting the legal authorization a carrier must have to conduct electronic surveillance, including section 2518(7) of Title 18 of the United States Code, which authorizes certain law enforcement personnel to conduct the interception of communications without a court order if an emergency situation exists involving:
  - (i) immediate danger of death or serious physical injury to any person,
  - (ii) conspiratorial activities threatening the national security interest, or
  - (iii) conspiratorial activities characteristic of organized crime.
- Affirmatively intervene to ensure that there is appropriate legal authorization for each electronic surveillance, including any appropriate authorization required under relevant state and federal statutes
- Give appropriate carrier authorization for the electronic surveillance
- Complete a certification form for each electronic surveillance he/she oversees and do so either contemporaneously with, or within a reasonable period of time after the initiation of, the surveillance.
- Ensure that records for each surveillance are placed in the appropriate secure files.

3. **T.E. Kloehr** shall ensure that this manual is updated and filed with the FCC within 90 days of any amendment of **Easytel Communications Carrier Corporation's** merger with another company.

III. GENERAL POLICIES FOR ELECTRONIC SURVEILLANCE, (CONT'D.)

D. Record keeping

An employee shall complete a certification form (sample attached as Appendix 1) for every electronic surveillance conducted on carrier premises – regardless of whether the surveillance was authorized or unauthorized.

Easytel Communications Carrier Corporation shall establish and label separate secure files in which it will retain all certification forms, court orders, and other records for (1) authorized call content interceptions; (2) unauthorized call content interceptions; and (3) authorized and unauthorized call information interception. These records shall be retained in secure and appropriately - marked secure files for **two (2) years** from the time the certification form is completed for the interception. It has been the custom and policy of **Easytel Communications Carrier Corporation** to maintain these records for this period of time, and experience has shown that this policy has adequately served the needs of **Easytel Communications Carrier Corporation** and law enforcement agencies.

E. Non-Disclosure of Contents of Authorized Surveillance; Unauthorized Surveillance and Compromises of Authorized Surveillance

Employees are prohibited from conducting any unauthorized surveillance and from disclosing to any person the existence of, the contents of, or information about, any law enforcement investigation or electronic surveillance, or the device used to accomplish such surveillance, unless required by legal process and then only after prior notification to a representative of the Attorney General of the United States or to the principal prosecuting attorney of the state or subdivision thereof, as may be appropriate.

Employees shall report any incidents of unauthorized surveillance and any compromises of authorized surveillance in accordance with the procedures in Section V of this manual.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE

A. Call Content Interceptions with a Title III Court Order

Step One: Any court order presented by a law enforcement agency for a call content interception pursuant to Title III shall be referred immediately to one of the employees designated in Section III.B of this manual.

Step Two: Before implementing the interception, or sending the request to the TTP, the designated employee shall ensure that the court order contains the following information:

(a) the identity of the person, if known, whose communications are to be intercepted;
(b) the nature and location of the communications facilities or the place for which authorized to intercept is granted;
(c) a particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates;
(d) the period of time during which the interception is authorized, including a statement whether the interception shall automatically terminate when the described communication has been first obtained;
(e) a provision that the authorization to intercept shall be executed as soon as practicable and conducted in such a way as to minimize the interception of communication not otherwise subject to interception;
(f) the identity of the agency authorized to intercept the communications and of the person authorizing the application; and
(g) the signature of a judge or magistrate.

Step Three: The designated employee also shall determine, or consult with the TTP to determine, whether the surveillance can be implemented technically and whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

A. Call Content Interceptions with a Title III Court Order, (Cont'd.)

Step Four: The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, or the TTP, but the designed employee shall continue to oversee the implementation of the surveillance.

Step Five: The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance or upon receipt of a certification form from the TTP. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order to the Certificate Form and sign the Certification form. The employee also shall attach to the Certification Form any extensions that are granted for the surveillance.

Step Six: The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate secure file.

Step Seven: The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates, or that the TTP terminates the surveillance, when the legal authorization expires. The interception shall be terminated at the time specified in the court order (which, in the absence of an extension, cannot exceed 30 days).

B. Call Content Interception Pursuant to Title III but *without* a Court Order

Step One: Any request by a law enforcement agency for a call content interception without a court order, pursuant to the exigent circumstance listed in 18 U.S.C § 2518(7), shall be referred immediately to one of the employees designated in Section III.B of this manual.

Step Two: Before implementing the interception, or sending the request to the TTP for implementation, the designated employee shall ensure that the law enforcement agency provides a certification containing the following information:

(a) the information, facilities, or technical assistance required;
(b) the period of time during which the provision of information, facilities, or technical assistance is authorized.
(c) a statement that no warrant or court order is required by law;
(d) a statement that all statutory requirement have been met;
(e) a statement that the specific requested assistance is required; and
(f) the signature of **either** (i) the Attorney General of the United States, or (ii) a law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

B. Call Content Interception Pursuant to Title III but *without* a Court Order, (Cont'd.)

Step Three: The designated employee also shall determine, or consult with the TTP to determine, whether the surveillance can be implemented technically and whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four: The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees or the TTP, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five: The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance or receipt of certification from the TTP. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.

Step Six: The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate secure file.

Step Seven: The designated employee shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance, or ensure the TTP terminates the surveillance, as soon as any of the following events occur:

(a) the law enforcement agency does not apply for a court order within 48 hours after the interception has begun; or
(b) the law enforcement agency's application for a court order is denied.

Step Eight: If the law enforcement agency does receive a court order for the surveillance, the designated employee shall validate the court order (as specified in Section IV.A, Step Two above), attach the order to the Certification form, and handle the surveillance in all respects under the procedures in Section IV.A.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

C. Call Information Interceptions using a Pen Register or Trap-and-Trace Device with a Court Order

Step One: Any court order presented by a law enforcement agency for a call information interception using a pen register or trap-and-trace device shall be referred immediately to one of the employees designated in Section III.B of this manual.

Step Two: Before implementing the interception, or sending the request to the TTP, the designated employee shall determine that the court order contains the following information:

(a) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap-and-trace device is to be attached;
(b) the identity, if known, of the person who is the subject of the criminal investigation;
(c) the number and, if known, physical location of the telephone line to which the pen register or trap-and-trace device is to be attached and, in the case of a trap-and-trace device, the geographical limits of the trap-and-trace order;
(d) a statement of the offense to which the information likely to be obtained by the pen register or trap-and-trace device relates; and
(e) the signature of a judge or magistrate.

Step Three: The designated employee also shall determine, or consult with the TTP to determine, whether the surveillance can be implemented technically and whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four: The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, or the TTP, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five: The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance or receipt of certification from the TTP. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order and sign the Certification Form. The employee also shall attach any extensions that are granted for the surveillance.

Step Six: The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate secure file.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

C. Call Information Interceptions using a Pen Register or Trap-and-Trace Device with a Court Order, (Cont'd.)

Step Seven: The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates, or that the TTP terminates the surveillance, when the legal authorization expires. The designated employee shall terminate the surveillance at the time specified in the order (which, in the absence of an extension, cannot exceed 60 days).

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

D. Call Information Interceptions using a Pen Register or Trap-and-Trace Device *without* a Court Order

Step One: Any request by a law enforcement agency for a call content interception without a court order, pursuant to the exigent circumstance listed in 18 U.S.C §3125 shall be referred immediately to one of the employees designated in Section III.B of this manual.

Step Two: Before implementing the interception or sending the request to the TTP, the designated employee shall ensure that the law enforcement agency provides a certification containing the following information:

(a) the information, facilities, or technical assistance required;
(b) the period of time during which the provision of information, facilities, or technical assistance is authorized;
(c) a statement that no warrant or court order is required by law;
(d) a statement that all statutory requirement have been met;
(e) a statement that the specific requested assistance is required; and
(f) the signature of a law enforcement officer specially designated by the Attorney General of the United State, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, and acting Assistant Attorney General, any Deputy Assistant Attorney, or by the principal prosecuting attorney of any state or subdivision thereof.

Step Three: The designated employee also shall determine, or consult with the TTP to determine, whether the surveillance can be implemented technically and whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four: The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees or the TTP, but the designated employee shall continue to oversee the implementation of the surveillance.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

D. Call Information Interceptions using a Pen Register or Trap-and-Trace Device *without* a Court Order, (Cont'd.)

Step Five: The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance or receipt of certification from the TTP. The employee shall supply all information requested on the Certification form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the certification Form.

Step Six: The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate secure file.

Step Seven: The designated employee shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance, or ensure the TTp terminates the surveillance, as soon as any of the following events occur:

(a) the information sought is obtained;
(b) the law enforcement agency's application for the court order is denied or 48 hours have lapsed since the installation of the device, whichever is earlier.

Step Eight: If the law enforcement agency does receive a court order for the surveillance, the designated employee shall validate the court order (as specified in Section IV.C, Step Two above), attach the order to the Certification Form, and handle the surveillance in all respects under the procedures in Section IV. C.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

E. Electronic Surveillance with a Foreign Intelligence Surveillance Act ("FISA") Court Order

Step One: Any court order presented by a law enforcement agency for electronic surveillance pursuant to FISA shall be referred immediately to one of the employees designated in Section III.B of this manual.

Step Two: Before implementing the interception or sending the request to the TTP, the designated employee shall ensure that the court order contains the following information:

(a) the identity, if known, or a description of the target of the electronic surveillance;
(b) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;
(c) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
(d) the means by which the electronic surveillance will effected and whether physical entry will be used to effect the surveillance;
(e) the period of time during which the electronic surveillance is approved;
(f) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device;
(g) a statement directing that the minimization procedure be followed;
(h) a statement directing that, upon the request of the applicant, a specified carrier furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that the carrier is providing that target of electronic surveillance;
(i) a statement directing that the carrier maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain;
(j) a statement directing that the applicant compensate, at the prevailing rate, the carrier for furnishing the aid; and
(k) the signature of a federal district judge designated pursuant to 50 USC §1803.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

E. Electronic Surveillance with a Foreign Intelligence Surveillance Act ("FISA") Court Order, (Cont'd.)

Whenever the target of the electronic surveillance is a foreign power (as defined under FISA) and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the court order need not contain the information required by subparagraphs (c), (d), and (f), but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

Step Three: The designated employee also shall determine, or consult with the TTP to determine, whether the surveillance can be implemented technically and whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four: The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees or the TTP, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five: The designated employee shall complete a Certification form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance, or upon receipt of certification from the TTP. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order and sign the Certification Form. The employee also shall attach and extensions that are granted for the surveillance.

Step Six: The designated employee shall ensure that the Certification form and all attachments are placed in the appropriate secure file.

Step Seven: The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates, or that the TTP terminates the surveillance, when the legal authorization expires. The interception shall be terminated at the time specified in the order. In the absence of an extension, the surveillance cannot exceed 90 days (or 1 year if the surveillance is targeted against a foreign power).

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

F. Electronic Surveillance Conducted Pursuant to FISA but without a Court Order

Step One: Any request by a law enforcement agency for electronic surveillance pursuant to FISA but without a court order shall be referred immediately to one of the employees designated in Section III.B of this manual.

Step Two: Although FISA does not expressly list the items which must be contained in the Attorney :General's certification, the designated employee shall ensure that the law enforcement agency provides a certification containing the following information before implementing the request or sending the request to the TTP:

(a) the information, facilities, or technical assistance required;
(b) the period of time during which the provision of information, facilities, or technical assistance is authorized;
(c) a statement that no warrant or court order is required by law;
(d) a statement that all statutory requirements have been met;
(e) a statement that the specific requested assistance is required; and
(f) the signature of the Attorney General of the United States, or his designee.

Step Three: The designated employee also shall determine, or consult with the TTP to determine, whether the surveillance can be implemented technically and whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four: The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, or the TTP, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five: The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance, or upon receipt of certification from the TTP. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.

Step Six: The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate secure file.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE, (CONT'D.)

F. Electronic Surveillance Conducted Pursuant to FISA but without a Court Order, (Cont'd.)

Step Seven: The designated employee shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance, or ensure the TTP terminates the surveillance, as soon as any of the following events occur:

(a) the information sought is obtained;
(b) the law enforcement agency's application or a court order is denied; or
(c) 24 hours have elapsed since the authorization of the surveillance by the Attorney General without the granting of a court order.

Step Eight: If the law enforcement agency does receive a court order for the surveillance, the designated employee shall validate the court order as specified in Section IV. E, Step Two above), attach the order to the Certification Form, and handle the surveillance in all respects under the procedures in Section IV.E.

V. PROCEDURES IF UNAUTHORIZED SURVEILLANCE OR A COMPROMISE OF SURVEILLANCE HAS OCCURRED

Step One: If any employee becomes aware of any act of unauthorized electronic surveillance or any compromise of authorized surveillance to unauthorized persons or entities, that employee shall promptly notify the individual(s) designated in Section III.B of this manual of the incident. Acting with legal counsel, the designated employee shall determine which law enforcement agencies are affected and promptly notify the agencies of the incident.

Step Two: The designated employee shall compile a certification record for any unauthorized surveillance and ensure that all records available to the carrier regarding the surveillance are placed in the appropriate carrier secure files.

APPENDIX 1

Certification Form for Electronic Surveillance Implemented By Easytel Communications Carrier Corporation.

INSTRUCTIONS: The information requested below shall be provided either on this form or by attaching the appropriate legal authorization for the surveillance if the authorization contains that information. If the authorization is attached, check the box below and attach any extensions that are granted for the surveillance.

I have attached a court order or other legal authorization for this surveillance as well as any extensions that have been granted.

1. Telephone number (s) and / or circuit identification numbers involved.	
2. Start date and time of the opening of the circuit for law enforcement.	
3. Law enforcement officer presenting the authorization.	
4. Person signing the appropriate legal authorization.	
5. Type of interception or access (e.g., pen register, trap and trace, Title III, FISA).	
6. Carrier employee responsible for overseeing the interception or access in accordance with the carrier's CALEA policies.	

I, _____, have overseen the electronic surveillance described on this form and on any attached documents, and I hereby certify that the information contained on this form and the attached documents is complete and accurate.

Signed: _____ **Date:** _____